6.

OUT OF SIGHT AND OUT OF MIND

The absolute importance of submarine cables to New Zealand

Phil Holdstock & John Moremon

New Zealanders depend on a critical communications infrastructure that few ever think about. Most of us are familiar with the internet and are accustomed to such terms as cyberspace, the cloud, 3G, 4G and 5G, but many of us may think our ability to complete everyday online tasks such as banking, emailing, social media, news and streaming is the result of something that happens 'up there' thanks to satellites and Wi-Fi. The truth is that our internet experience is shaped by a more mundane yet incredibly sophisticated technology: a worldwide network of copper and fibre-optic cables buried underground on land and laid across ocean floors. This cable network carries a staggering 95–99 per cent of global electronic communications — and includes more than 1 million kilometres of undersea submarine cables.[1]

The lack of public awareness of this infrastructure is not unique to New Zealand. Even though submarine cables are laid across almost every ocean and sea, connecting virtually every continental and island state, scholars have noted that it 'remains surprising how little is known in public or among policymakers about how the network operates, how it is regulated, who controls it, and how it is protected from vulnerabilities'.[2]

This lack of awareness stems from a 'triple invisibility'. First, as a society, we tend to take for granted most forms of infrastructure, such

ProtectingAotearoa_TEXT_MV5.indd 97 10/10/23 3:00 PM

as roads, buildings, sewers and cables, until something goes wrong. Second, cables are out of sight, with perhaps the only visual clue to their existence in our lives being the easy-to-ignore flashing lights on the ONT (Optical Network Terminal, aka modem) inside our home or business. And third, not only is most of the cable network under the surface, but most of it is in the darkest depths of the ocean.[3] Despite their lack of visibility, however, submarine cables are vital to our national prosperity and security. In essence, submarine cables provide the physical bedrock of cyberspace and the cloud and thus play a tremendous part in our social connectedness and contributions to global governance and the global economy.[4]

New Zealand's geographic location as an island nation in the south of the South Pacific means that submarine cables are critically important. However, although New Zealand has legislation to protect submarine cables in its territorial waters from accidental or deliberate damage, most are foreign-owned, outside territorial waters, and facing an array of potential military, terrorist and natural threats. As Rishi Sunak noted before he became British prime minister, submarine cables can be summed up with two words: 'indispensable, insecure'.[5] The importance of submarine cable networks is such that they must be factored into public dialogue and decision-making around national and international security.

THE USE OF CABLES FOR governmental, commercial and social communication goes as far back as the 1840s. Following the invention of electromagnetic telegraphy, vast networks of above-ground copper lines were constructed on continents and large islands, and telegraph operators used Morse code to send and receive messages. Postal mail services were important, but the telegraph enabled faster delivery of messages and faster responses.[6] From the outset, cables tended to be laid and owned by companies rather than governments, thus avoiding the political friction that could come from having telegraph cables linking different countries. To this day, commercial entities are responsible for most cable development. However, despite their private appearance and legal status, 'international telecommunications companies have almost always been hybrid creatures: private in appearance and by law, but intimately tied to their home governments'.[7]

The earliest cable networks were on land, but people soon realised that sending telegraph messages across the seas would also be advantageous and profitable. The first undersea cable was laid across the English Channel in 1850–51, and during 1854–58 a submarine cable was laid across the Atlantic Ocean, connecting Europe and North America. This transatlantic cable failed after three weeks. However, even in that short time it proved its worth, allowing for investment to produce a cable able to withstand oceanic conditions. Further submarine cables were laid across important passages, including the Mediterranean and the Red Sea, and in 1865–66 another was laid across the Atlantic.[8]

The submarine cable networks offered tremendous commercial and social benefits. However, they were also strategically important, being more secure than overland lines and less troublesome diplomatically, as cables could be laid across oceans and seas without negotiating with foreign governments. From the 1870s, Britain supported laying an extensive submarine cable network, the All-Red Line, to service the British Empire. With security front of mind, the route of the All-Red Line was planned to avoid foreign soil as much as possible, only coming ashore on islands or continental coastlines of the British Empire or close allies. Royal Navy warships would patrol sea lanes over the cables, and defences were constructed at relay stations where the cables come ashore.[9] The 1884 Convention for the Protection of Submarine Telegraph Cables meanwhile compelled signatory states (even to this day) to enact laws making it an offence to wilfully or negligently break or damage a submarine cable, or to interfere with the activities of cable-laying and cable-repair ships.[10]

New Zealand's first submarine cable was laid in 1866 between Lyall Bay in the North Island and Whites Bay in the South Island to connect the domestic telegraph network. In 1876 the first trans-Tasman cable, between Botany Bay near Sydney and Cable Bay near Nelson in the South Island, was completed, with another then laid from Cable Bay to Whanganui to connect with the North Island. The trans-Tasman cable was a technological marvel, in places 5 kilometres deep and strung across undersea mountains, canyons and plains, despite the fact that deep ocean surveying was not possible at that time.

In 1902 a New Zealand branch of the British-American Pacific cable (part of the All-Red Line) was laid between Doubtless Bay in Northland

and Norfolk Island, from where lines ran west to Brisbane, north to Hawai'i and on to Vancouver, Canada.[11] These cables gave New Zealand direct connections to Australia and indirect connections to Asia, North America and Europe. The communications infrastructure was strategically, commercially and socially significant, allowing messages to be sent between governments, militaries, businesses and families around the world in peacetime and in wartime.

IN THE MID-TWENTIETH CENTURY, SUBMARINE telegraph cables experienced a decline in use due to the introduction of new technologies, including wireless (radio) transmission from the 1930s. In the 1950s new submarine coaxial telephone cables were laid, but they proved technologically challenging and expensive and offered limited bandwidth. As a result, by the 1970s most transoceanic communications traffic was carried by satellites.[12]

New Zealand became part of the 'space age' in 1965 when the first satellite call was made between Britain and New Zealand, and in 1971 the opening of Warkworth Satellite Earth Station, north of Auckland, enabled the use of satellites for television broadcasts.[13]

A more far-reaching development occurred in 1986 when the University of Waikato connected to the world wide web via a dial-up telephone connection. As internet technology and accessibility developed, in 1989 New Zealand became the first country in the Asia-Pacific region to connect to the United States' internet backbone; 1193 New Zealand customers were connected in the first two years. This grew to 15,000 in the following two years — globally the fastest growth rate in internet accessibility.[14]

The renewed focus on submarine cables came about because the satellite network was inadequate for the increased data traffic generated by the internet. High-bandwidth fibre-optic cables provided the solution. The growth of the internet and the laying of fibre-optic submarine cables have gone hand-in-hand since the 1990s: 'In essence, the two technologies complemented each other perfectly: cables carried large volumes of voice and data traffic with speed and security; the internet made that data and information accessible and useable for a multitude of purposes.'[15]

In fact, there has never been another period when submarine cables

have been more significant to humanity. Global connectivity depends on some 450 submarine cable networks worldwide with a total undersea cable length of over 1 million kilometres. Low-orbit satellites have started to take some of the load from the local fibre-optic networks; indeed, New Zealand mobile providers have begun to utilise the Starlink satellite network. However, even with the move to using satellites, the submarine cables remain crucial, linking the satellite ground stations to data storage and providing the critical commercial links between countries. Christian Bueger and Tobias Liebetrau argue that submarine cable networks should not be seen merely as data transmission conduits but rather as 'an economic trade route carrying the most important commodity of the information age: data'.[16]

The 1982 United Nations Convention on the Law of the Sea (UNCLOS) allows governments and companies to maintain existing submarine cable networks and lay new networks in non-territorial waters without requiring environmental impact studies. Studies by the United Nations Environment Programme, the World Conservation Monitoring Centre, the International Cable Protection Committee (a non-profit member organisation that promotes the security of cable networks) and research teams from other organisations have, in any case, found that modern submarine cables have a neutral to minor impact on the marine environment.[17]

In recent years there has been significant investment from an array of communications companies and content giants, all free to pursue the growth of submarine cable networks. Collectively, Google, Meta, Amazon and Microsoft make up four-fifths of recent investment in submarine cables, although competition from Chinese companies is increasing rapidly, particularly in the Indo-Pacific region.[18]

THE SUBMARINE CABLE INFRASTRUCTURE THAT serves New Zealand has continued to grow exponentially. The Southern Cross fibre-optic cable connecting Hawai'i to Takapuna was completed in 2000 and rapidly reduced the country's reliance on satellite communications.[19] Domestically, in the late 1990s and early 2000s, the Aqua Link network was laid along the coastlines of the northeastern South Island and western North Island to link main centres. In the last decade a second loop link of the Southern Cross Cable was laid from Whenuapai to

Hawai'i; another connection to Hawai'i is provided by the Hawaiki Cable spur connected to Mangawhai Heads. In addition, the Tasman Global Access Cable connects Raglan and Sydney.[20] The latest submarine cable connected to New Zealand is a spur of the Southern Cross Next cable, which in July 2022 linked Takapuna and Los Angeles (with connections to Australia, Fiji and Kiribati); this cable alone doubled New Zealand's data transmission capacity.[21]

The New Zealand activity is essential but pales in comparison to the global race to develop submarine cable networks, especially across the Atlantic, Indian and Pacific oceans. On top of American commercial interest in developing new networks and hubs, China intends to lay networks across the Indian and Pacific oceans as a digital extension ('a digital Silk Road') of China's Belt and Road Initiative.[22]

The developing networks influence New Zealand's commerce, security and society both directly and indirectly: without access to the internet provided by submarine cable networks, it would be impossible for the country to transmit and receive vast amounts of data generated in real time. To give one indication of the importance of the digital link, New Zealand's banks belong to the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which links 8300 banking members in 195 economies; every day, SWIFT is responsible for US$10 trillion in financial transfers and over 15 million financial messages: most of this is transmitted using cable networks.[23] While New Zealand's share of SWIFT communications is modest, the ability to link with such networks is of fundamental importance.

The significance of the submarine cable infrastructure to the country cannot be underestimated. Yet, this critical infrastructure is still often overlooked in broader public discussions of New Zealand's security interests.

AS NOTED AT THE OUTSET, submarine cables are 'out of sight and out of mind' for most New Zealanders. At governmental and intergovernmental levels there is awareness of the submarine cable network and the array of security threats, as demonstrated in policies and agreements at these levels. For example, in 2018, as part of the Pacific Islands Forum, New Zealand signed the Boe Declaration on regional security. While most attention has been given to the declaration's affirmation that climate

change is the primary threat to the livelihoods in the Pacific, it also acknowledges the vulnerability of member states to threats to their security, with an intention to 'maximise the protection and opportunities for Pacific infrastructure and peoples in the digital age'.[24] It is impossible to achieve regional security in the digital age without considering the submarine cable network.

New Zealand has appropriate legislation that specifically covers the security of submarine cables in its territorial waters with the Submarine Cables and Pipelines Protection Act 1996, as required under the 1884 Convention for the Protection of Submarine Telegraph Cables, of which New Zealand is a signatory. This is concerned principally with the types of physical threats from shipping activities that existed when the convention was drafted in the early 1880s.[25] Under this Act, New Zealand has 10 declared Cable Protection Areas (in areas of Great Barrier Island, Hauraki Gulf, Kawau Island, Whangaparāoa Peninsula, Muriwai Beach, Taharoa, Cook Strait, Oaonui, Hawke's Bay and in Taranaki around the Maui A and B gas pipelines) where anchoring and most types of fishing are banned.[26] But the Act does not address modern challenges such as the physical distance required between the now greater number of submarine cables in congested sea spaces, co-location with other activities such as undersea mining and fisheries, cybersecurity threats or natural threats.[27]

SUBMARINE CABLES FACE AN ARRAY of threats attributable to three leading causes: negligence, intentional damage or destruction, and natural events. While there is no cable damage reporting requirement, worldwide some 150–200 faults affecting submarine cables occur annually, of which fewer than 10 per cent result from natural hazards. Some 65–75 per cent of damage events occur mainly as a result of fishing and shipping activities, in areas where water depth is 200 metres or less. In much deeper waters, natural hazards become the primary cause of damage: approximately 31 per cent of faults in deep water are traceable to natural events, 14 per cent to fish bites on cables, and 28 per cent to unknown causes.[28]

The military use of submarine cables was not considered initially, despite the military achievements during the Crimean War of 1853–56. The British Colonial Office's Colonial Defence Committee recognised the cable vulnerabilities in the nineteenth century, and the 1884 Convention

for the Protection of Submarine Telegraph Cables sought to deal with the most obvious form of physical threat: accidental physical damage. As noted, New Zealand's Submarine Cables and Pipelines Protection Act 1996 seeks to provide the grounds for prosecution in the event of such damage in territorial waters. However, there is a more sinister possibility of deliberate human interference that may be harder to counter.

The vulnerability of submarine cables to foreign interference was realised during the early twentieth century. The first significant deliberate attack on a submarine cable occurred within hours of the start of the First World War when British forces cut all but one of Germany's transatlantic cables; they left one intact to allow codebreakers to intercept and read messages.[29] Similar action was taken early in the Second World War. Then in 1971, at the height of the Cold War (1947–91), the United States began tapping into Soviet-owned submarine cables for intelligence gathering. These episodes established a practice of sabotage and espionage that continues today in various forms. In recent years there has been a small number of reported physical attacks on, and interference with, submarine cables, ranging from criminal theft of cable components to state-sponsored sabotage and cyberattacks by different groups.[30]

In 2014, documents leaked by Edward Snowden highlighted that the US National Security Agency had implemented a metadata collection programme, codenamed Speargun, in which New Zealand's Government Communications Security Bureau (GCSB) played a supporting role. According to the leaked documents, Five Eyes partners regularly use surveillance probes to tap into fibre-optic cables to gather information deemed to be of importance for international and national security.[31]

Given the rising superpower tensions in the Asia-Pacific region, the prevalence of transnational crime and the potential for terrorism, the vulnerability of submarine cables is a genuine concern. Military, terrorist or criminal physical attacks have the capacity to damage or cripple submarine cable networks.

Cyberattacks pose another serious threat, with the possibility of states, criminal groups or hostile groups hacking into network management systems to seize control of transmissions, skim personal and financial information transmitted over the cables, or mount ransom attacks. The US Department of Homeland Security thwarted at least one serious cyberattack on a submarine cable network in April 2022,

although it could not confirm the attacker or the motivation.[32] Countries like New Zealand, which rely heavily on foreign-owned submarine communication infrastructure for economic and national security, may be impacted directly or indirectly by any of these forms of attack on the cable infrastructure. The GCSB is likely to play a further role in securing submarine cables serving New Zealand.

The vulnerability of submarine cables was brought to the attention of politicians in 2017 when Rishi Sunak, then a British member of parliament and now British prime minister, released a discussion paper, *Undersea Cables*, arguing that submarine cables are vitally important for international communications but are 'inherently vulnerable', and explaining that 'their location is generally publicly available, they tend to be highly concentrated geographically both at sea and on land, and it requires limited technical expertise and resources to damage them'.[33]

Sunak also warned of potential Russian aggression, and discussed how Russia's hybrid warfare model extends to utilising sabotage to destabilise an adversary's communications. Indeed, this occurred as part of Russia's invasion and annexation of Crimea in 2014: Russia cut the submarine cable that linked mainland Ukraine and the Crimean Peninsula, which enabled it to control the flow of information (and disinformation) concerning the invasion. Furthermore, Russia, and possibly other countries too, has invested in deep-sea submersibles and intelligence-gathering ships that can attack undersea infrastructure, including pipelines and submarine cables. Unfortunately, existing laws of armed conflict and laws of the sea do not provide robust protection for submarine cables.[34]

Rising tensions in the Asia-Pacific also open the possibility of hybrid warfare in this region, including potentially state-sanctioned attacks on South Pacific communications networks, which would threaten the interests of New Zealand and other South Pacific nations. The undersea infrastructure is mainly foreign-owned, particularly American-owned, and most cables terminate at four chokepoint locations: Sydney, Hawai'i, Guam and Los Angeles.[35]

While much of the cable network rests at depths where direct physical interference is not likely or possible, shallower waters and any locations where cables come ashore are points of physical vulnerability. Potential threats include disguised ships loitering in shallow waters and

using submersibles to cut cables, or the worst-case scenario of missile or air strikes on key communication hubs.[36] As China gains influence across the Asia-Pacific region, it gains greater access to critical infrastructure in the area, including points where cables are accessible on land.

The United States (and no doubt its Five Eyes partners) monitors the situation, including reviewing ownership of critical infrastructure, intending to mitigate threats.[37] Future state or non-state sabotage, espionage, military attack or cyberattack against cable networks could potentially leave New Zealand with only an indirect submarine cable route via Sydney, either temporarily or for some duration. If the Sydney connections were also compromised, it would severely disrupt New Zealand's communications capability.[38] While a direct military attack on cable locations seems unthinkable, as it would mean a war had broken out, we should be aware of the inherent vulnerabilities built into the submarine cable networks.

There is, in addition, an ever-present natural threat to submarine cables — the potential for damage from natural events particularly evident within the Pacific's Ring of Fire, where triggering events include volcanic eruptions, earthquakes, tropical and sub-tropical cyclones and typhoons. These events can cause strong turbidity currents that result in underwater landslides. The impact of such events was illustrated in December 2006 when a magnitude 7.0 earthquake occurred off southern Taiwan, triggering a series of underwater landslides that produced dense sediment-laden turbidity currents that fell rapidly to the ocean floor, breaking nine fibre-optic submarine cables. The event seriously impacted Southeast Asia's regional and global communications, including telephone, internet and other data-transfer services.[39]

Recently, the January 2022 eruption of the Hunga-Tonga-Hunga-Ha'apai underwater volcano off Tonga showed clearly the vulnerability of the cables in our region. The eruption shredded 80 kilometres of submarine cables, making the repair mission far more complex than a simple cut from an anchor or fishing equipment, as might occur in shallower waters. The reinstatement of the undersea cable took five weeks, including two weeks to get a repair vessel to the location.[40]

Recent natural disasters have shown in stark detail the vulnerability of New Zealand's communications infrastructure. Cyclone Gabrielle in 2023 caused widespread damage across the North Island, damaging power-

lines, fibre cable networks and mobile phone networks on land, isolating towns and rural communities and hindering emergency services. The loss of electronic payment systems and internet access caused disruptions to local commerce and economies and highlighted what can happen when communication infrastructure is impacted or compromised.[41] Significantly, the cyclone struck at a point where three submarine cable landing sites are located, and while on this occasion damage to submarine cable infrastructure was avoided, the event should serve as a reminder of the potential for damage from serious storms and flooding.

In the past when the locations of cable landing stations were chosen, no thought was given to accelerated climate change and its effects on coastal environments. Cable hubs in many countries tend to be located on low coastal ground, and many land-based cables are in low-lying coastal zones. Possible future responses to the climate change threat may include enhanced monitoring of storm-surge predictions, relocating cable stations if necessary, and developing back-up systems to ensure that networks can continue to operate if a cable network is damaged.[42]

New Zealand can, in fact, start to mitigate the impact of infrastructure loss by planning to relocate cable infrastructure and potentially add government-owned low-level communication satellites to provide additional redundancy pathways. Using satellites for redundancy for New Zealand has become a viable option because the launching facilities at Māhia Peninsula are significantly cheaper to use than traditional launching sites.[43] Ulrich Speidel suggests also increasing the resilience of New Zealand's communications infrastructure by having a back-up microwave capability between mobile phone towers, with satellite use ensuring sustained connections in times of emergency. However, while the emerging low-level satellite networks can play a part in national and regional responses to local disasters, they do not have the capability to make the submarine cable networks redundant.[44]

IN THE MODERN AGE, CLOUD computing is synonymous with global connectivity. While submarine cables may appear archaic, they are essential to modern life and serve as the backbone of the internet. These cables link countries to create, in effect, a submarine web; however, like a giant spider web, the infrastructure is vulnerable to threats, including natural disasters, accidental damage and deliberate interference.

The South Pacific region presents unique challenges for laying and maintaining submarine cables due to its location within the Ring of Fire and its transformational boundary, which makes the region prone to seismic and volcanic events. Climate change threatens further significant risks, as rising sea levels can affect landing stations and onshore cables connected to the submarine cables. Great power competition, rising geostrategic tensions, transnational crime and the ever-present potential for terrorism mean that the submarine cables are also susceptible to human interference.

These vulnerabilities are significant because of the critical nature of the infrastructure, particularly for New Zealand, which relies heavily on submarine cables for global communications and connectivity. Protecting these cables must be considered a national security issue, and steps must be taken to ensure resilience in the face of the array of potential threats. However, this will require sustained government action.

It would be timely for the New Zealand government and private sector entities to publicly assess the threats to submarine cable networks, ahead of investing in back-up systems and developing protocols for expeditious and effective responses in the event of serious damage to a network or networks. This may include consideration of active steps that can be taken to improve national and regional responses, such as maintaining regional stocks of spares for the repair of damaged cables, and providing input into the strengthening of national and international legal frameworks required to enhance the protection of submarine cables against such threats as hybrid warfare, cyber warfare and criminal activity.

The inherent vulnerability and criticality of submarine cables for global and national communications make it imperative to take these steps both for New Zealand and its Pacific partners. By understanding and acknowledging the vulnerabilities in the infrastructure and implementing appropriate measures, we can mitigate the risks and ensure that the submarine cables remain a reliable and secure resource for as long as they are needed. It is critical that we act to protect the submarine cables against the array of threats to ensure that in the event of a failure, an incredible technological innovation does not become our undoing.

6. Out of sight and out of mind

1 Lionel Carter et al., *Submarine Cables and the Oceans: Connecting the world* (Cambridge & Lymington: United Nations Environmental Programme World Conservation Monitoring Centre and the International Cable Protection Committee, 2009), 3; Frank Rose, 'Emerging threats: Outer space, cyberspace, and undersea cables', *Arms Control Today*, January/February 2017, www.armscontrol.org/act/2017-01/news/remarks-emerging-threats-outer-space-cyberspace-undersea-cables
2 Christian Bueger & Tobias Liebetrau, 'Protecting Hidden Infrastructure: The security politics of the global submarine data cable network', *Contemporary Security Policy* 42, no. 3 (2021): 392, https://doi.org/10.1080/13523260.2021.1907129
3 Ibid., 393–94.
4 Utpal Kumar Raha & K. D. Raja, *Submarine Cables Protection Regulation: A comparative analysis and model framework* (Singapore: Springer, 2021), 1.
5 Rishi Sunak, *Undersea Cables: Indispensable, insecure* (London: Policy Exchange, 2017).
6 Roland Wenzlhuemer, *Connecting the Nineteenth-century World: The telegraph and globalization* (Cambridge: Cambridge University Press, 2012), 30–58.
7 David R. Headrick & Pascal Griset, 'Submarine Telegraph Cables: Business and politics, 1838–1939', *The Business History Review* 75, no. 3 (Autumn 2001): 544.
8 Simone M. Müller, *Wiring the World: The social and cultural creation of global telegraph networks* (New York: Columbia University Press, 2016), 19–47.
9 P. M. Kennedy, 'Imperial Cable Communications and Strategy, 1870–1914', *The English Historical Review* 86, no. 341 (1971): 729–31.
10 Tara Davenport, 'Submarine Cables, Cybersecurity and International Law: An intersectional analysis', *Catholic University Journal of Law and Technology* 24, no. 1 (2017): 6–67.
11 Jeffrey K. Lyons, 'The Pacific Cable, Hawaii, and Global Communication', *The Hawaiian Journal of History* 39 (2005): 35–42.
12 Keith Lewis, 'Engineering on the Sea Floor — Submarine cables', *Te Ara: The Encyclopedia of New Zealand*, https://teara.govt.nz/en/engineering-on-the-sea-floor; Carter et al., *Submarine Cables and the Oceans*, 14–15.
13 Ministry for Culture and Heritage, 'Warkworth Satellite Earth Station', NZ History, https://nzhistory.govt.nz/media/photo/warkworth-satellite-earth-station
14 Keith Newman, *Connecting the Clouds: The internet in New Zealand* (Auckland: Activity Press, 2008), https://www.nethistory.co.nz/Chapter_6_-_Craving_for_Connection
15 Carter et al., *Submarine Cables and the Oceans*, 16.
16 Bueger & Liebetrau, 'Protecting Hidden Infrastructure', 405.
17 Douglas R. Burnett & Lionel Carter, *International Submarine Cables and Biodiversity of Areas Beyond National Jurisdiction: The cloud beneath the sea* (Leiden and Boston: Brill, 2017), 54–55, https://doi.org/10.1163/24519359-12340002
18 Hilary McGeachy, 'The Changing Strategic Significance of Submarine Cables: Old technology, new concerns', *Australian Journal of International Affairs* 76, no. 2 (2022): 164–66; Bueger & Liebetrau, 'Protecting hidden infrastructure', 405.
19 Ministry for Culture and Heritage, 'Warkworth Satellite Earth Station'.
20 George H. Seltzer et al., 'New Zealand's Aqualink Network: A submarine solution for domestic high-speed infrastructure', 2001, https://cdn.b12.io/client_media/n8KzZTRM/59d857a4-d2e9-11eb-945e-0242ac110003-Aqualink_01.pdf; TeleGeography, 'Submarine cable map', www.submarinecablemap.com/; Winston Qui, 'Raglan Cable Landing Station', Submarine Cable Networks, 30 September 2020, www.submarinenetworks.com/en/stations/oceania/new-zealand/raglan
21 Daniel Smith, 'Oceanic cable to double New Zealand's internet capacity launches from Auckland', *Stuff*, 29 June 2021, www.stuff.co.nz/business/300344613/oceanic-cable-to-double-new-zealands-internet-capacity-launches-from-auckland
22 Hong Shen, 'Building a Digital Silk Road? Situating the internet in China's Belt and Road Initiative', *International Journal of Communication* 12 (2018): 3683.
23 Christof Gerlach & Richard Seitz, *Economic Impact of Submarine Cable Disruptions* (Singapore: APEC Policy Support Unit, 2013), 9.
24 'Boe Declaration on Regional Security', Pacific Islands Forum, 2018, www.forumsec.org/2018/09/05/boe-declaration-on-regional-security
25 Karen Scott, 'Laws governing undersea cables have hardly changed since 1884 — Tonga is a reminder they need modernising', *The Conversation*, 21 January 2022, https://

theconversation.com/laws-governing-undersea-cables-have-hardly-changed-since-1884-tonga-is-a-reminder-they-need-modernising-175312
26 'Protecting New Zealand's undersea cables', Te Manatū Waka Ministry of Transport, www.transport.govt.nz/about-us/what-we-do/queries/protecting-new-zealands-undersea-cables
27 Scott, 'Laws governing undersea cables have hardly changed since 1884'.
28 Carter et al., *Submarine Cables and the Oceans*, 39.
29 Kennedy, 'Imperial Cable Communications and Strategy', 729–31; Elizabeth Bruton, 'The Cable Wars: Military and state surveillance of the British telegraph cable network during World War One', in Andreas Marklund & Mogens Rüdiger (eds), *Historicizing Infrastructure* (Aalborg: Aalborg University Press, 2017), 5–6.
30 Congressional Research Service, 'Undersea Telecommunication Cables: Technology overview and issues for Congress', CRS Report R47237 (Washington, DC: Congressional Research Service, 2022), 11–13.
31 Philip Dorling, 'Edward Snowden reveals tapping of major Australia–New Zealand undersea telecommunications cable', *Sydney Morning Herald*, 15 September 2014, www.smh.com.au/technology/edward-snowden-reveals-tapping-of-major-australianew-zealand-undersea-telecommunications-cable-20140915-10h96v.html
32 Congressional Research Service, 'Undersea Telecommunication Cables', 13.
33 Sunak, *Undersea Cables*, 19.
34 Dennis E. Harbin III, 'Targeting Submarine Cables: New approaches to the law of armed conflict in modern warfare', *Military Law Review* 229, no. 3 (2021): 351.
35 TeleGeography, 'Submarine cable map'.
36 Sebastian Moss, 'Fortune on the High Seas — DCD', Datacenter Dynamic, 2016, www.datacenterdynamics.com/en/analysis/fortune-on-the-high-seas
37 Jonathan E. Hillman, *The Digital Silk Road: China's quest to wire the world and win the future* (London: Profile Books, 2021), 107.
38 TeleGeography, 'Submarine cable map'.
39 Carter et al., *Submarine Cables and the Oceans*, 9.
40 Ulrich Speidel, 'The Hunga Tonga Hunga Ha'apai Eruption — a Postmortem: What happened to Tonga's internet in January 2022, and what lessons are there to be learned?', *AINTEC 2022* (Association for Computing Machinery: 18–21 December 2022), 75; Tom Bateman, 'Tonga is finally back online: Here's why it took 5 weeks to fix its volcano-damaged internet cable', *Euronews*, 23 February 2022, www.euronews.com/next/2022/02/23/tonga-is-finally-back-online-here-s-why-it-took-5-weeks-to-fix-its-volcano-damaged-interne
41 Ulrich Speidel, 'Cyclone Gabrielle broke vital communication links when people needed them most — what happened and how do we fix it?', *New Zealand Herald*, 3 March 2023, www.nzherald.co.nz/nz/cyclone-gabrielle-broke-vital-communication-links-when-people-needed-them-most-what-happened-and-how-do-we-fix-it/22NDWWPKMZEKDIQWCP6566X2UQ
42 Ramakrishnan Durairajan, Carol Barford & Paul Barford, 'Lights Out: Climate change risk to internet infrastructure', *ANRW 2018* (Association for Computing Machinery: 16 July 2018), 9–15.
43 Deloitte Access Economics, *New Zealand Space Economy: Its value, scope and structure* (Wellington: Ministry of Business, Innovation and Employment, November 2019), www.beehive.govt.nz/sites/default/files/2019-11/Deloitte NZ Space Economy Report.pdf
44 Speidel, 'Cyclone Gabrielle broke vital communication links when people needed them most'.

7. Outlaw motorcycle gangs and the illegal drug trade

1 Jarrod Gilbert, *Patched: The history of gangs in New Zealand* (Auckland: Auckland University Press, 2013); Gregory D. Breetzke et al., 'Gang Membership and Gang Crime in New Zealand: A national study identifying spatial risk factors,' *Criminal Justice and Behavior* (2021): 1154–72; Anusha Bradley, 'Gangs of New Zealand: Explosion of violence prompts fears police have lost control', 23 March 2020, *The Guardian*, www.theguardian.com/world/2020/mar/23/gangs-of-new-zealand-explosion-of-violence-prompts-fears-police-have-lost-control; New Zealand Parliamentary Services, 'New Zealand gang membership: A snapshot of recent trends', July 2022, www.parliament.nz/media/9557/gangs-in-nz-snapshot-july-2022.pdf
2 Anna Leask, 'Organised crime evolving "rapidly" in NZ as borders become "porous" to illicit trade', 15 October 2019, *New Zealand Herald*, www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12276597; Breetzke et al., 'Gang membership', 1154;